SPYWOLF

Security Audit Report

Completed on

September 21, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **Operation Rise** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Operation Rise

PROJECT DESCRIPTION

According to their whitepaper:

Operation Rise is a crypto currency token aimed at supporting communities of crypto scams by air-dropping free tokens as part of their 'Rug Relief' mechanism.

Their future development phases will involve the launch of own NFT marketplace, featuring sets of Operation Rise NFTs with some collections being able to be used in the upcoming play to earn game, as well as 1,000s of others.

Release Date: Presale starts on Sep, 2022

Category: P2E/NFT

CONTRACT 1 INFO

Token Name
OperationRise

Symbol
OpRise

Contract Address
0xEaEad1c7BA9129507F8aB29136370d03AB6c49dd

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Aug 20, 2022

Verified?
Yes

Total Supply
100,000,000

Status
Not launched

TAXES

Buy Tax
15%

Sell Tax
15%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of Sept 21, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

No limit

DEX:

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	100000000 OpRise
Median Transfer Amount	100000000 OpRise
Average Transfer Amount	100000000 OpRise
First transfer date	2022-08-20
Last transfer date	2022-08-20
Days token transferred	1

SMART CONTRACT STATS

Calls Count	7
External calls	7
Internal calls	0
Transactions count	7
Uniq Callers	1
Days contract called	1
Last transaction time	Aug-20-2022 01:45:28 AM +UTC
Created	Aug-20-2022 01:12:19 AM +UTC
Create TX	0x7d87f3c9716f27dd25e98d889a183bd7ba53405ecb7ec9c0ba3cd71d889dc3f9
Creator	0x2218fb301d2fea1e870e9c15a853852806b09daf

FEATURED WALLETS

Owner address	0x9c61b58f959c9645ef6060c91412e7090e9afa84
Buy fee recipient	0xbcf2e24a4d47d5dfdff0955a465c89fd6a74009a
Sell fee recipient	0xc5ddb4cc9f6dd0fe1f6e93000d8d06912302ea18
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1

100% Same as owner

*Tokens are not distributed yet

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

If distributor address is set to inappropriate contract or externally owned account (wallet), buys and sells will fail.

```
function setDistributor(address newDistributor) external onlyOwner {
    distributor = IDistributor(newDistributor);
    emit SetDistributor(newDistributor);
}
```

FOUND THREATS

⚠ Medium Risk

Owner can set buy/sell/transfer fees up to 25%.
Combined buy+sell=50%.

```
function setFees(uint _buyFee, uint _sellFee, uint _transferFee) external onlyOwner {
    require(
        _buyFee <= 2500,
        'Buy Fee Too High'
    );
    require(
        _sellFee <= 2500,
        'Sell Fee Too High'
    );
    require(
        _transferFee <= 2500,
        'Transfer Fee Too High'
    );

    buyFee = _buyFee;
    sellFee = _sellFee;
    transferFee = _transferFee;

    emit SetFees(_buyFee, _sellFee, _transferFee);
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

Informational

Owner can withdraw any tokens from contract.

```
function withdraw(address token) external onlyOwner {
    require(token != address(0), 'Zero Address');
    bool s = IERC20(token).transfer(msg.sender, IERC20(token).balanceOf(address(this)));
    require(s, 'Failure On Token Withdraw');
}

function withdrawBNB() external onlyOwner {
    (bool s,) = payable(msg.sender).call{value: address(this).balance}("");
    require(s);
}
```

Owner can exclude address from fees.

```
function setFeeExempt(address account, bool isExempt) external onlyOwner {
    require(account != address(0), 'Zero Address');
    permissions[account].isFeeExempt = isExempt;
    emit SetFeeExemption(account, isExempt);
}
```

CONTRACT 2 INFO

Token Name	Symbol
OpRise Rewards	opBNB

Contract Address
0xA02d4a2B9414917420D4f35884161b2DE60D00cB

Network	Language
Binance Smart Chain	Solidity

Deployment Date	Verified?
Aug 20, 2022	Yes

Total Supply	Status
N/A	Deployed

TAXES

Buy Tax	Sell Tax
n/a	n/a

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

FEATURED WALLETS

Owner address	0x9c61b58f959c9645ef6060c91412e7090e9afa84

FOUND THREATS

⚠ High Risk

The following functions can be called by anyone, exposing the contract to DDOS attacks.

```
function massClaim() external {
    _massClaim(0, allUsers.length);
}

function massClaimFromIndexToIndex(uint256 startIndex, uint256 endIndex) external {
    _massClaim(startIndex, endIndex);
}
```

Looping large arrays could lead to denial of service.

```
function _massClaim(uint256 startIndex, uint256 endIndex) internal {
    require(
        endIndex <= allUsers.length,
        'End Length Too Large'
    );

    for (uint i = startIndex; i < endIndex;) {
        _sendReward(allUsers[i]);
        unchecked { ++i; }
    }
}
```

- Recommendation:
  - Restrict access to external functions and reduce the possible iterations through array.

Informational

Owner can withdraw any tokens from contract.

```
function withdraw(address _token, uint256 amount) external onlyOwner {
    IERC20(_token).transfer(msg.sender, amount);
}

function withdrawBNB(uint256 amount) external  onlyOwner {
    (bool s,) = payable(msg.sender).call{value: amount}("");
    require(s);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Operation Rise

GOOD PRACTICES FOUND

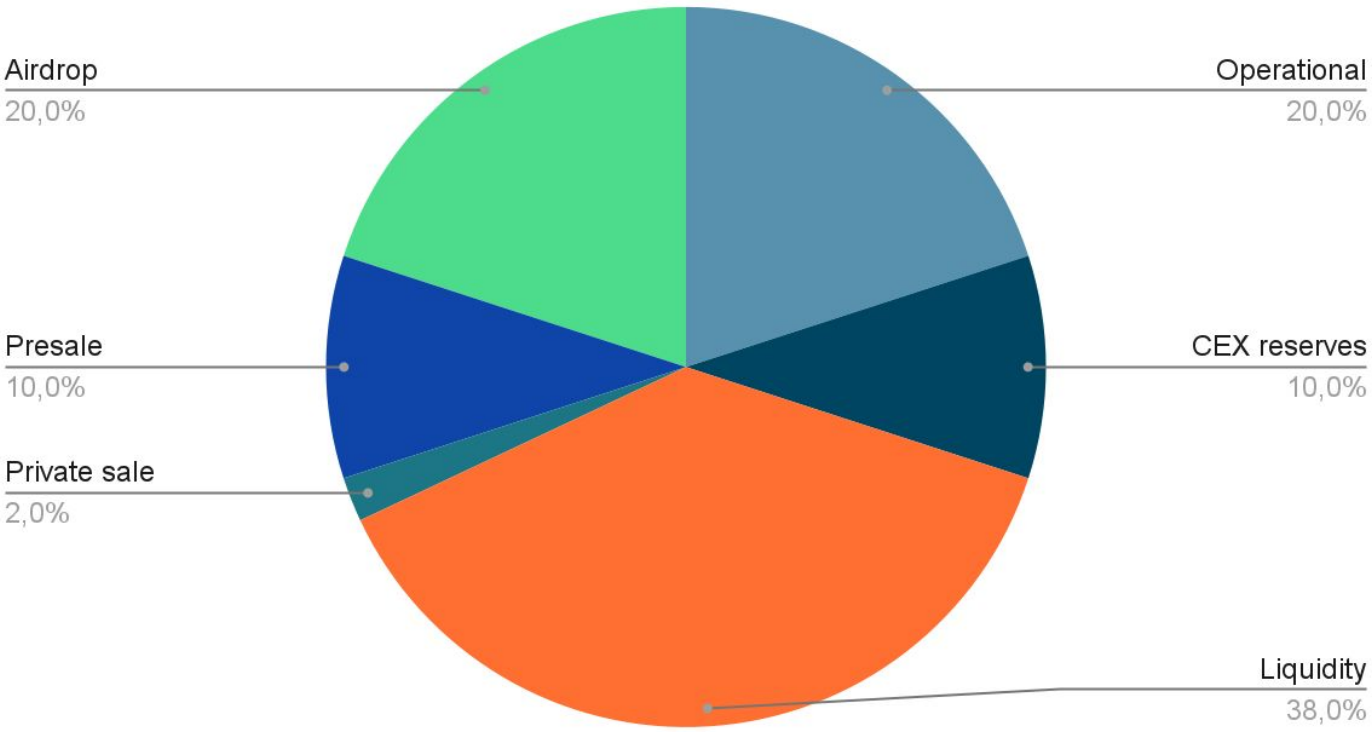
- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

*The following tokenomics are based on the project's whitepaper and/or socials:

- 20% - Operational (OpRise LLC)
- 10% - Locked for CEX
- 38% - Liquidity
- 10% - Presale
- 2% - Private sale
- 20% - Airdrop

Tokens distribution



THE TEAM

The team has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members KYC'd

KYC Date

September 22, 2022

Format

Image

Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/September_2022/KYC_OperationRise_0xEaEad1c7BA9129507F8aB29136370d03AB6c49dd.png

WEBSITE

Website URL
https://www.operation-rise.com/

Domain Registry
https://www.wix.com

Domain Expiration
Expires on 2023-02-13

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

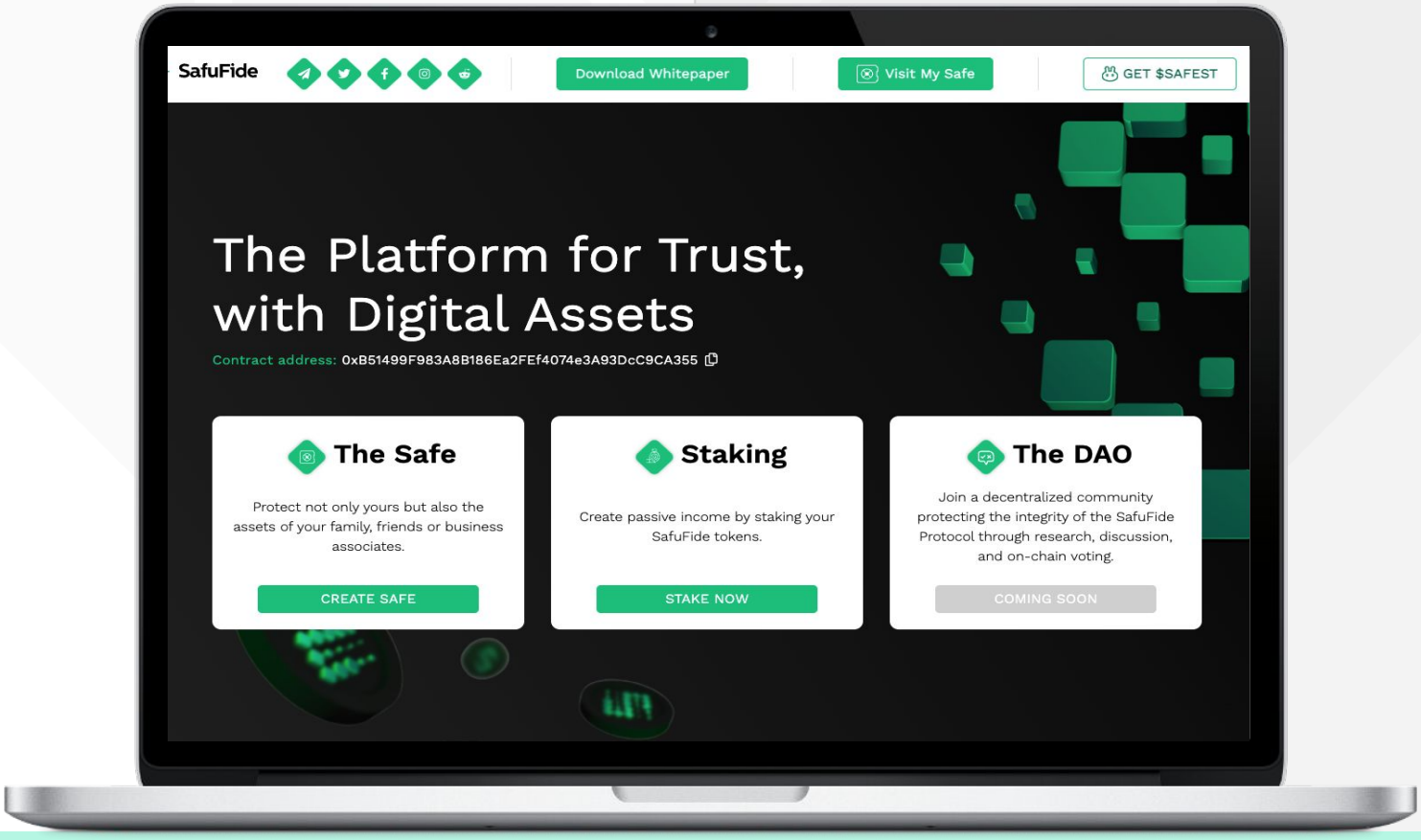
Design
Appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set at 4 phases without time frames.

Mobile-friendly?
No

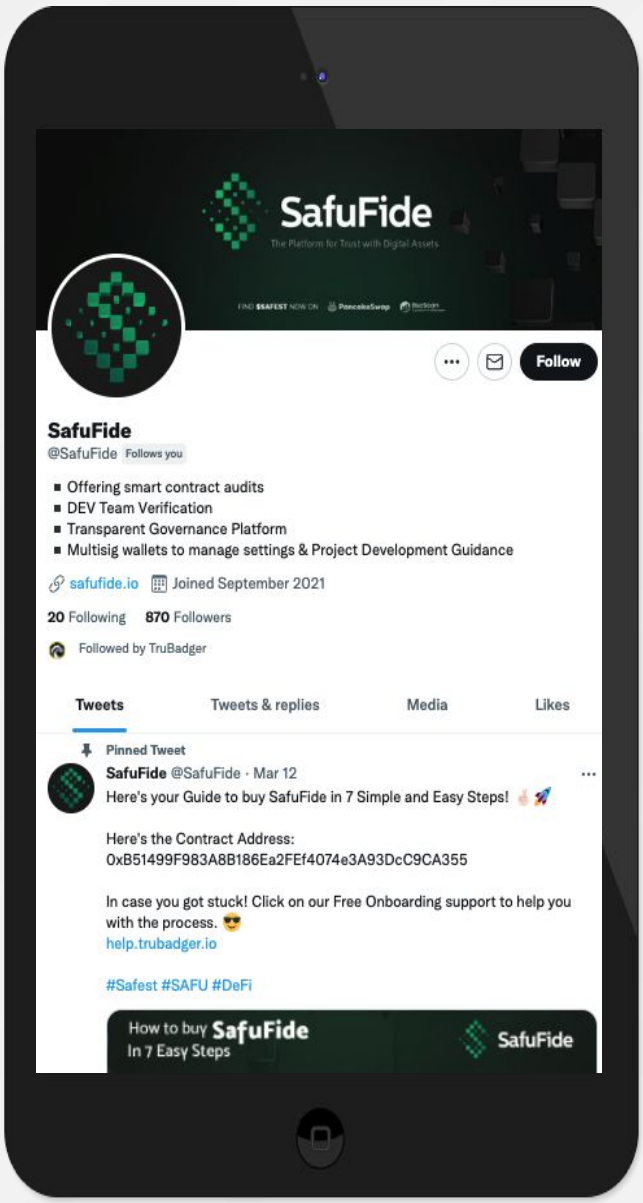


operation-rise.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS



Twitter

@operation_rise_

- 201 followers
- ⚠️Not very active - since month of may, posts once every few weeks.

Discord

- Not available

Telegram

@TelegramUSERNAME

- 200 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.